State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

September 2, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2015-104

DATE ISSUED:
09/02/2015

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, which could result in arbitrary code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
• Google Chrome prior to version 45.0.2454.85
• Google V8 prior to version 4.5.103.29

RISK:
Government:
• Large and medium government entities: High
• Small government entities: High
Businesses:
• Large and medium business entities: High
• Small business entities: High
Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Google Chrome. These vulnerabilities can be triggered by a user visiting a specially crafted web page. Details of these vulnerabilities are as follows:
•   A cross-origin policy bypass exists due to an error with DOM. (CVE-2015-1291, CVE-2015-1293)
•   A cross-origin policy bypass exists due to an error with ServiceWorker. (CVE-2015-1292)
•   A use-after-free vulnerability exists due to an error in Skia. (CVE-2015-1294)
•   A use-after-free vulnerability exists due to an error in Printing. (CVE-2015-1295)
•   A character spoofing vulnerability exists due to an error in omnibox. (CVE-2015-1296)
•   A security vulnerability exists due to permission scoping error in WebRequest. (CVE-2015-1297)
•   A URL validation vulnerability exists due to an error in extensions. (CVE-2015-1298)
•   A use-after-free vulnerability exists due to an error in Blink. (CVE-2015-1299)
•   An information-disclosure vulnerability exists in Blink. (CVE-2015-1300)
•   Multiple security vulnerabilities exist due to certain unspecified errors. (CVE-2015-1301)
•   Multiple security vulnerabilities exist in V8 due to certain unspecified errors.

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
We recommend the following actions be taken:
•   Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
•   Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
•   Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
•   Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Google:
http://googlechromereleases.blogspot.com/2015/09/stable-channel-update.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1295
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1296
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1297
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1298
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1299
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1300
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1301